ABSTRACT OF THE DISCLOSURE

An autonomous and portable smartcard reader device incorporates a high level of embedded security countermeasures. Data transfers are encrypted with two specific input devices, namely a light sensor and PIN or other keyboard entry, and at the output through the use of a dual-tone encoder-decoder. The unit may be used alone or as a plug-in to another device such as a PDA, cell phone, or remote control. The reader may further be coupled to various biometric or plug-in devices to achieve at least five levels of authentication, namely, (1) the smartcard itself; (2) the smartcard reader; (2) the PIN; (3) private-key cryptography (PKI); and (5) the (optional) biometric device. These five levels account for an extremely strong authentication applicable to public networking on public/private computers, and even on TV (satellite, cable, DVD, CD AUDIO, software applications. Transactions including payments may be carried out without any risk of communication tampering, authentication misconduct or identity theft. In essence, the device is a closed box with only two communication ports. The emulation of the device is therefore extremely complex due to the fact that it involves PKI and or identity-based encryption (IBE), key pair, elliptic curves encryption scheme, hardware serialization for communication and software implementation, in conjunction with a specific hardware embodiment and service usage infrastructure component that returns a response necessary for each unique transaction.